Michal Křížek; Jan Chleboun
A note on factorization of the Fermat numbers and their factors of the form
$3h2^n + 1$


Persistent URL: [http://dml.cz/dmlcz/126115](http://dml.cz/dmlcz/126115)

**Terms of use:**

© Institute of Mathematics AS CR, 1994

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*
A NOTE ON FACTORIZATION OF THE FERMAT NUMBERS
AND THEIR FACTORS OF THE FORM $3h2^n + 1$

MICHAŁ KRÍŽEK, JAN CHEBOUN, Praha

(Received May 9, 1994)

Summary. We show that any factorization of any composite Fermat number $F_m = 2^{2^m} + 1$ into two nontrivial factors can be expressed in the form $F_m = (k2^n + 1)(\ell2^n + 1)$ for some odd $k$ and $\ell$, $k \geq 3$, $\ell \geq 3$, and integer $n \geq m + 2, 3n < 2^m$. We prove that the greatest common divisor of $k$ and $\ell$ is 1, $k + \ell \equiv 0 \mod 2^n$, max$(k, \ell) \geq F_{m-2}$, and either $3 \mid k$ or $3 \mid \ell$, i.e., $3h2^{m+2} + 1 \mid F_m$ for an integer $h \geq 1$. Factorizations of $F_m$ into more than two factors are investigated as well. In particular, we prove that if $F_m = (k2^n + 1)^2(\ell2^n + 1)$ then $j = n + 1, 3 \not\mid \ell$ and $5 \not\mid \ell$.

Keywords: Fermat numbers, prime numbers, factorization, squarefreeness

AMS classification: 11A51, 11Y05

Throughout the paper all variables $i, j, k, n, n_1, \ldots$ are supposed to be positive integers except for $m$ and $z$ which can moreover attain the value zero. For $m = 0, 1, 2, \ldots$, the $m$th Fermat number is defined by $F_m = 2^{2^m} + 1$. The aim of this paper is to derive some properties of factors of composite Fermat numbers.

Recall that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are primes and other primes $F_m$ (if they exist) are not known yet. For instance, in 1732 Euler found that $F_5 = 641 \cdot 6700417$, where the both factors are prime. The Fermat number $F_6$ was factored by Landry in 1880 (see e.g. [10]), $F_7$ by Morrison and Brillhart in 1970 [8], $F_8$ by Brent and Pollard in 1980 [2], $F_9$ by Lenstra, Lenstra, Jr., Manasse, Pollard in 1990 [7] and $F_{11}$ by Brent in 1988 [1]. The complete factorizations of $F_m$ are known only for the above mentioned numbers for the time being. Their structure, however, remains a deterministic chaos. Some prime factors of $F_{10}$ and of more than 100 other Fermat numbers can be found in excellent surveys [3, 6]. From all of the above-mentioned papers we have

(1) \[ 1 = \Omega_0 = \ldots = \Omega_4 < 2 = \Omega_5 = \ldots = \Omega_8 < 3 = \Omega_9 < 5 = \Omega_{11} < 6 < \Omega_{12}, \]
where \( \Omega_m \) is the number of prime divisors of \( F_m \) (counted with multiplicity). Anyhow, the monotonicity of the whole sequence \( \{\Omega_m\} \) is an open problem as well as the squarefreeness of \( F_m \).

In 1877, Lucas established a general form of prime divisors of the Fermat numbers, namely that: Every prime divisor \( p \) of \( F_m, m > 1 \), satisfies the congruence (see e.g. [4, p. 376])

\[
p \equiv 1 \mod 2^{m+2}.
\]

The main idea of its proof is the following. As in [7, p. 320] we put \( b = 2^{2^m-2} (2^{2^m-1} - 1) \). Then \( b^2 = 2^{2^m-1} (2^{2^m} - 2 \cdot 2^{2^m-1} + 1) \) and we get

\[
b^2 \equiv 2 \mod p,
\]

since \( 2^{2^m} + 1 \equiv 0 \mod p \). From here we have \( b^{2^m+1} \equiv 2^{2^m} \equiv -1 \mod p \) which implies that

\[
b^{2^{m+2}} \equiv 1 \mod p.
\]

According to (3), the numbers \( b \) and \( p \) are coprime and thus by the little Fermat theorem (i.e., \( b^{p-1} \equiv 1 \mod p \)) and (4) it is possible to deduce that \( 2^{m+2} | p - 1 \). Therefore, (2) holds.

We start with several simple lemmas.

**Lemma 1.** If \( 2^n + 1 \) divides \( F_m \) for some \( n \geq 1 \) and \( m \geq 0 \) then \( F_m = 2^n + 1 \).

**Proof.** Set \( Q_n = 2^n + 1 \), i.e., \( F_m = Q_{2^m} \). From the binomial theorem we obtain

\[
Q_{ij} = 2^{ij} + 1 = (Q_j - 1)^i + 1 \equiv 1 + (-1)^i \mod Q_j
\]

and thus

\[
\gcd(Q_{ij}, Q_j) = \begin{cases} 
1 & \text{for } i \text{ even,} \\
Q_j & \text{for } i \text{ odd.}
\end{cases}
\]

Hence,

\[
\gcd(F_z, F_m) = 1 \quad \text{for } z \neq m,
\]

i.e., no two different Fermat numbers have a common divisor greater than 1 (see also [5, p. 14]).

Suppose that \( Q_n | F_m \) for some \( n < 2^m \). Then \( n = i2^z \), where \( i \) is odd and \( z < m \). Using (5) for \( j = 2^z \), we see that \( Q_{2^z} | Q_n \). However, this contradicts (6), since \( Q_{2^z} = F_z \) and \( Q_n | F_m \). Therefore, \( n = 2^m \). \( \square \)
Lemma 2. Let $F_m$ be composite. Then there exist natural numbers $j, k, \ell, n$ such that

(7) \[ F_m = (k2^n + 1)(\ell2^j + 1), \quad k \geq 3, \ell \geq 3, k \text{ and } \ell \text{ are odd.} \]

Proof. Since $F_m$ is odd and composite, it can be written as a product of two odd numbers $k2^n + 1$ and $\ell2^j + 1$ for some natural numbers $n, j$ and odd integers $k, \ell$. However, according to Lemma 1 the case $k = 1$ or $\ell = 1$ is not possible. Hence, $k \geq 3$ and $\ell \geq 3$. \hfill \Box

Definition 3. Let $q > 1$ be an odd integer. A uniquely determined exponent $n$ from the decomposition $q = k2^n + 1$, where $k$ is odd, is called the order of $q$.

In the next lemma we prove that the orders of two odd factors are not greater than the order of their product.

Lemma 4. Let

(8) \[ k2^n + 1 = (k_12^{n_1} + 1)(k_22^{n_2} + 1), \]

where $k, k_1, k_2$ are odd. Then $n \geq \min(n_1, n_2)$, where the sharp inequality holds if and only if $n_1 = n_2$. Moreover, $k > k_1k_22^{\max(n_1, n_2)}$ whenever $n_1 \neq n_2$.

Proof. Without loss of generality assume that $n_1 \geq n_2$. Then

(9) \[ k2^n + 1 = (k_1k_22^{n_1} + k_12^{n_1-n_2} + k_2)2^{n_2} + 1. \]

Since $k$ is odd, $n \geq n_2 = \min(n_1, n_2)$. The number in the brackets from (9) is even if and only if $n_1 = n_2$. If $n_1 > n_2$ then $n = n_2$ and thus $k > k_1k_22^{n_1}$ by (9). \hfill \Box

Theorem 5. Let $F_m$ be composite and let $k2^n + 1$ be its arbitrary factor (not necessarily prime) where $k$ is odd. Then $k \geq 3$, $n$ is an integer for which

(10) \[ m + 2 \leq n < \frac{1}{3}2^n \]

and there exists an odd $\ell \geq 3$, such that

(11) \[ F_m = (k2^n + 1)(\ell2^n + 1), \]

i.e., the both factors have the same order. Moreover,

(12) \[ k + \ell \equiv 0 \mod{2^n}, \]
and \( k \) and \( \ell \) are coprime, i.e.,

\[
\begin{align*}
(13) \quad & \gcd(k, \ell) = 1, \\
(14) \quad & \max(k, \ell) \geq F_{m-2}
\end{align*}
\]

and

\[
(15) \quad \text{either } 3 \mid k \text{ or } 3 \mid \ell,
\]

i.e., for any composite Fermat number \( F_m \) there exists a natural number \( h \) such that \( 3h2^n + 1 \mid F_m \).

Proof. Let \( \ell 2^j + 1 \) be a cofactor to \( k 2^n + 1 \) such that \( \ell \) is odd. According to (7), we have

\[
F_m = k\ell 2^{n+j} + k 2^n + \ell 2^j + 1.
\]

Without loss of generality we may assume that \( n \geq j \). Then

\[
2^{2^{m-j}} = k\ell 2^n + k 2^{n-j} + \ell,
\]

where the terms \( 2^{2^{m-j}} \) and \( k\ell 2^n \) are even because \( 2^m > j \) and \( n \geq 1 \). This implies that \( n = j \), since \( \ell \) is odd. (The role of \( k \) and \( \ell \) is thus the same.)

From the relation

\[
2^{2^n-n} = k\ell 2^n + k + \ell,
\]

we deduce that \( 2^m - n > n \) which implies (12). Moreover, if \( q \mid k \) and \( q \mid \ell \) for some odd \( q \) then \( q \mid 2^{2^n-n} \). Hence, \( q = 1 \) and we observe that (13) holds.

Further we establish the proposed bounds (10) for \( n \). By (12), \( k + \ell \geq 2^n \). Since \( k \neq \ell \) due to (13), we have

\[
\begin{align*}
(16) \quad & \max(k, \ell) > 2^{n-1},
\end{align*}
\]

and thus

\[
F_m = (k 2^n + 1)(\ell 2^n + 1) > (2^{n-1} 2^n + 1)(2 \cdot 2^n + 1) > 2^{3n} + 1.
\]

Consequently, \( 3n < 2^m \).

By (2) each prime factor of \( F_m \) is of the form \( r 2^{m+2} + 1 \) for some integer \( r \).
Hence, if \( k 2^n + 1 \) is a prime factor then \( m + 2 \leq n \), since \( k \) is odd. Suppose that \( k 2^n + 1 \) is a product of two primes which is of the form (8). Then Lemma 4 implies \( m + 2 \leq \min(n_1, n_2) \leq n \). By induction we find that \( m + 2 \leq n \) for any factor of \( F_m \), i.e., (10) is valid.
If \( n \leq 2^{m-2} \) then by (11), (13) and (10)
\[
\max(k, \ell) > 2^{-n}(\sqrt{F_m - 1}) > 2^{-2^{m-2}}(2^{2^{m-1}} - 1) = 2^{2^{m-2}} - 2^{-2^{m-2}}
\]
and thus \( \max(k, \ell) > F_{m-2} \), since \( \max(k, \ell) \geq 2^{2^{m-2}} \) and \( k \) and \( \ell \) are odd. Conversely, if \( n \geq 2^{m-2} + 1 \) then by (16),
\[
\max(k, \ell) > 2^{n-1} \geq 2^{2^{m-2}}
\]
i.e., (14) holds.

Finally we prove (15). Obviously,
\[
3 \mid 2^n + (-1)^{n+1}.
\]
Hence, \( 3 \mid F_m - 2 \) (taking \( n = 2^m \)) and thus \( (k2^n + 1)(\ell2^n + 1) \equiv 2 \mod 3 \). This and (17) imply
\[
(1 + (-1)^n)k)(1 + (-1)^n) \equiv 2 \mod 3.
\]
We easily find that \( xy \equiv 2 \mod 3 \) if and only if \( x \equiv 2 \mod 3 \) and \( y \equiv 1 \mod 3 \) or \( x \equiv 1 \mod 3 \) and \( y \equiv 2 \mod 3 \). From here and (18) we observe that just one of the numbers \( k \) and \( \ell \) is divisible by 3. \( \square \)

**Corollary 6.** Let the assumptions of Theorem 5 be satisfied and let \( 3 \mid \ell \). Then
\[
(19) \quad k = 3u + 1 \quad \text{for some } u \text{ even} \iff n \text{ is even},
\]
\[
(20) \quad k = 3u + 2 \quad \text{for some } u \text{ odd} \iff n \text{ is odd}.
\]

**Proof.** As \( 3 \mid \ell \), we have from (15) that \( k = 3u + y, 1 \leq y \leq 2 \) and from (18)
\[
1 + (-1)^n k \equiv 2 \mod 3.
\]
This yields (19) and (20). \( \square \)

**Remark 7.** Although the upper bound on \( n \) in (10) is too rough, we observe that no \( n \) satisfies (10) if \( m \leq 4 \) (which implies that \( F_0, \ldots, F_4 \) are primes without carrying out any trial divisions). For the prime factor 641 = \( 5 \cdot 2^7 + 1 \) of \( F_5 \) we have the equality \( n = m + 2 \). On the other hand, the sharp inequality \( n > m + 2 \) holds e.g. for the factorization of \( F_8 \) into two primes with \( n = 11 \). By (11) and (10)
\[
\min(k, \ell) < (2^n \min(k, \ell) + 1)/2^n < \sqrt{F_m}/2^n < F_{m-1}/2^{m+2}.
\]
Moreover, \( \min(k, \ell) \geq 3 \), where the equality is achieved e.g. for prime factors of \( F_{38} \) and \( F_{207} \) (see [3, p. lxxxviii]). According to (11) and (13), no Fermat number is a square of a natural number.
Theorem 8. Let \( n_1 \leq n_2 \leq n_3 \) and let

\[
F_m = \prod_{j=1}^{3} (k_j 2^n + 1),
\]

where \( k_j \) are odd. Then \( k_j \geq 3 \) for \( j = 1,2,3, \ldots \), and the trivial fact that \( F_m = 7 \) mod 10 for \( m > 1 \), we have \( k_3 2^{n_3} + 1 \) mod 10 \( \in \{3, 7\} \) which yields \( 5 \not| k_3 \).

\[ \square \]
Remark 9. The Fermat number $F_9$ is a product of three prime factors $k_j 2^{n_j} + 1$, $j = 1, 2, 3$, cf. (1). According to [7, p. 321], their orders are $n_1 = n_2 = 11 = m + 2$ and $n_3 = 16$ and thus by (11), we get

$$F_9 = (k_1 2^{11} + 1)(k_2 2^{11} + 1) = (k_3 2^{16} + 1)(k_3 2^{16} + 1)$$

for some $\ell_j \geq 3$ odd. Hence, any factor $\ell 2^n + 1$ of $F_m$ for which $n = m + 2$ need not be a prime factor yet. We also see that for given $n \geq m + 2$ the Diophantine equation (11) with unknowns $k$ and $\ell$ can have no or one or more solutions. It is also interesting that no $k_j$ from (24) is divisible by 3. This can be directly verified from the explicit expressions of the prime factors of $F_9$ (see [7]) and thus $3 \mid \ell_j$ for $j = 1, 2, 3$ by (15). According to (22), no Fermat number is a cube of a natural number.

**Theorem 10.** Let $n_1 \leq n_2 \leq \ldots \leq n_N$, $N > 1$ and let

$$F_m = \prod_{j=1}^{N} (k_j 2^{n_j} + 1),$$

where $k_j$ are odd. Then $m + 2 \leq n_j$, $k_j \geq 3$ for $j = 1, \ldots, N$, and the number of factors $k_j 2^{n_j} + 1$, whose order is $n_1$, is even. No two factors from (25) form a twin prime pair.

**Proof.** We again have by Theorem 5 that $m + 2 \leq n_j$ and $k_j \geq 3$ for all $j = 1, \ldots, N$. For $N < 4$ the proof of the first part of Theorem 10 follows from Theorems 5 and 8. So let $N \geq 4$. Suppose, on the contrary, that $2z + 1$ (for an integer $z \geq 0$) is the number of factors of the lowest order $n_1$, i.e., $n_{2z+1} < n_{2z+2}$ if $2z + 1 < N$. Then by Lemma 4 we have for $z \geq 1$ that

$$\text{ord}((k_{2i} 2^{n_1} + 1)(k_{2i+1} 2^{n_1} + 1)) > n_1 \quad \text{for any } i = 1, \ldots, z,$$

where analogously to [7, p. 321] the operator ord denotes the order from Definition 3, i.e., $\text{ord}(k 2^n + 1) = n$ for $k$ odd. Using Lemma 4 again, we find by induction that

$$\text{ord} \left( \prod_{j=2}^{2z+1} (k_j 2^{n_1} + 1) \right) > n_1$$

and thus also

$$\text{ord} \left( \prod_{j=2}^{N} (k_j 2^{n_j} + 1) \right) > n_1$$
for $z \geq 1$. However, we easily find that (26) holds even if $z \geq 0$. This contradicts (25) and (11), as $\text{ord}(k_i 2^{n_i} + 1) = n_1$.

Let $n_j \leq n_i$. Then

$$|(k_i 2^{n_i} + 1) - (k_j 2^{n_j} + 1)| = |(k_i 2^{n_i-n_j} - k_j)2^{n_j}| \geq 2^{n_j} \geq 2^{m+2}$$

whenever $n_i \neq n_j$ or $k_i \neq k_j$. From here we see that the product (25) cannot contain a twin prime pair. \hfill \Box

Remark 11. The 21-digit factor of $F_{11}$ (see [1]) is of order 14. The other four factors have order 13.

Two prime factors of $F_{10}$ are already known and their orders are 12 and 14 (see [3]). The associated cofactor is known to be composite, i.e., $\Omega_{10} = N \geq 4$, cf. (1) and (25). Note that the first prime factor of $F_{10}$ is of the form $k_1 2^{n_1} + 1 = 11131 \cdot 2^{12} + 1$.

By Theorem 10 there exists another prime factor of order $m + 2 = 12$, $k_2 2^{12} + 1$, $k_2 \geq 3$ odd, where $k_2$ is for the time being unknown. However, by (20) and (11), $k_2$ cannot be of the form $k_2 = 3v + 2$, since $n_2 = 12$ is even.

From Theorem 10 we observe that there exist at least four factors of $F_{12}$ of order $m + 2 = 14$, as three of them are already known [3].

Finally note that $k_j$ in (25) need not be coprime (cf. (13)). For instance we have $3 | k_j$ for two factors of $F_{11}$ and $7 | k_j$ for other its two factors, and $7 | k_j$ for three of the known factors of $F_{12}$, etc.

Acknowledgement. This research was supported by grant No. 201/94/1067 of the Grant Agency of the Czech Republic. The authors thank the referee for valuable suggestions and the reference [9].

References


444

Authors’ address: Michal Křížek, Jan Chleboun, Mathematical Institute, Academy of Sciences of the Czech Republic, Žitná 25, CZ-115 67 Prague 1, Czech Republic, e-mail: krizek@earn.cvut.cz, chleboun@earn.cvut.cz.